On a noncommutative reciprocity law

Igor Nikolaev *

Abstract

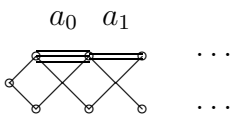
We prove a reciprocity relation, which says that an L-function of the noncommutative torus with real multiplication coincides with the Hasse-Weil L-function of an elliptic curve with complex multiplication. Our proof is based on an explicit formula for the Teichmüller functor between elliptic curves and noncommutative tori. The result entails, that the Cuntz-Krieger algebras are isomorphic to elliptic curves over finite fields.

Key words and phrases: elliptic curves, noncommutative tori

AMS Subj. Class.: 11G15; 46L85

Introduction

A. Real multiplication. Let $0 < \theta < 1$ be an irrational number; consider an AF-algebra, $\mathbb{A}_\theta$, given by the following Bratteli diagram:



, where $\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}$

Figure 1: The AF-algebra $\mathbb{A}_\theta$.

The K-theory of $\mathbb{A}_\theta$ is (essentially) the same as for noncommutative torus, i.e. the universal C^*-algebra generated by the unitaries u and v satisfying the

*Partially supported by NSERC.

commutation relation $vu = e^{2\pi i\theta}uv$ [10]; for brevity, we call $\mathbb{A}_\theta$ a noncommutative torus. Two such tori are *stably isomorphic*, whenever $\mathbb{A}_\theta \otimes \mathcal{K} \cong \mathbb{A}_{\theta'} \otimes \mathcal{K}$, where $\mathcal{K}$ is the C^*-algebra of compact operators; the isomorphism occurs, if and only if, $\theta' = (a\theta + b)/(c\theta + d)$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$ [4]. The $\mathbb{A}_\theta$ is said to have *real multiplication*, whenever θ is a quadratic irrationality [7]; we shall denote such an algebra by $\mathbb{A}_{RM}$. The real multiplication is equivalent to the fact, that the ring $End\ (K_0(\mathbb{A}_\theta))$ exceeds $\mathbb{Z}$; here $K_0(\mathbb{A}_\theta) \cong \mathbb{Z} + \mathbb{Z}\theta$. Moreover, any $\mathbb{A}_{RM}$ has a periodic Bratteli diagram with the incidence matrix A; the latter is connected to θ by an explicit formula $A = \prod_{i=1}^{n}(a_i, 1, 1, 0)$, where $\theta = [\overline{a_1, \ldots, a_n}]$ is a purely periodic fraction. (Here a line notation for the matrices and the Lagrange's Theorem for the quadratic irrationalities have been tacitly used.)

B. The Teichmüller functor. let $\mathbb{H} = \{x + iy \in \mathbb{C} \mid y > 0\}$ be the upper half-plane and for $\tau \in \mathbb{H}$ let $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ be a complex torus; we routinely identify the latter with a non-singular elliptic curve via the Weierstrass $\wp$ function. Two complex tori are isomorphic, whenever $\tau' = (a\tau + b)/(c\tau + d)$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. If τ is imaginary and quadratic, the elliptic curve is said to have a *complex multiplication*; the latter is equivalent to the condition, that the ring of endomorphisms of lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ exceeds $\mathbb{Z}$. Such curves are fundamental in arithmetic algebraic geometry; we shall denote them by E_{CM}. There exists a continuous map, which maps isomorphic elliptic curves to the stably isomorphic noncommutative tori; an exact result is this. (We refer the reader to [9] for the details.) Let ϕ be a closed form on the topological torus, whose trajectories define a measured foliation; according to the Hubbard-Masur theorem (applied to the complex tori), this foliation corresponds to a point $\tau \in \mathbb{H}$. The map $F : \mathbb{H} \to \partial\mathbb{H}$ is defined by the formula $\tau \mapsto \theta = \int_{\gamma_2} \phi / \int_{\gamma_1} \phi$, where γ_1 and γ_2 are generators of the first homology of the torus. The following is true: (i) $\mathbb{H} = \partial\mathbb{H} \times (0, \infty)$ is a trivial fiber bundle, whose projection map coincides with F; (ii) F is a functor, which sends isomorphic complex tori to the stably isomorphic noncommutative tori. We shall refer to F as the *Teichmüller functor*. The Teichmüller functor maps each E_{CM} to a noncommutative torus $\mathbb{A}_{RM}$; the correspondence establishes an equivalence between the two categories, so that any arithmetical property of the E_{CM} transforms into such of the $\mathbb{A}_{RM}$, where it often takes a simpler form.

C. A localization problem. Let p be a prime number; denote by $E_{CM}(\mathbb{F}_\mathfrak{P})$ a localization of the E_{CM} at the prime ideal $\mathfrak{P}$ over p [11]. In this paper,

we seek a solution to the following problem: find a localization of the non-commutative torus $\mathbb{A}_{RM}$ at prime p corresponding to the $E_{CM}(\mathbb{F}_{\mathfrak{P}})$. Note, that such a solution involves the L-functions, since the cardinals $|E_{CM}(\mathbb{F}_{\mathfrak{P}})|$ generate the Hasse-Weil function $L(E_{CM}, s)$ of the E_{CM}; roughly speaking, we construct an L-function of the torus $\mathbb{A}_{RM} = F(E_{CM})$, which coincides with the Hasse-Weil function of E_{CM} (a *reciprocity law*). The L-function of $\mathbb{A}_{RM}$ is introduced as follows. Denote by L_p a positive integer matrix $\begin{pmatrix} tr\ (A^p) - p & p \\ tr\ (A^p) - p - 1 & p \end{pmatrix}$ and define an endomorphism of $\mathbb{A}_{RM}$ by the action of L_p on generators u and v of the torus. Consider a crossed product $\mathbb{A}_{RM} \rtimes_{L_p} \mathbb{Z}$ by the endomorphism, which is stably isomorphic to the Cuntz-Krieger algebra $\mathcal{O}_{L_p}$ [1], §10.11.9. For $z \in \mathbb{C}$ and $\alpha \in \{-1, 0, 1\}$ define

$$\zeta_p(\mathbb{A}_{RM}, z) := \exp\left(\sum_{n=1}^{\infty} \frac{|K_0(\mathcal{O}_{\varepsilon_n})|}{n}\ z^n\right),\ \varepsilon_n = \begin{cases} L_p^n, & \text{if } p \nmid tr^2(A) - 4 \\ 1 - \alpha^n, & \text{if } p \mid tr^2(A) - 4, \end{cases}$$

a *local* zeta function of the $\mathbb{A}_{RM}$. An *L-function* of the $\mathbb{A}_{RM}$ is a product of the local zetas over all primes: $L(\mathbb{A}_{RM}, s) = \prod_p \zeta_p(\mathbb{A}_{RM}, p^{-s}), s \in \mathbb{C}$. Our main result is the following

Theorem 1 *$L(\mathbb{A}_{RM}, s) \equiv L(E_{CM}, s)$, where $\mathbb{A}_{RM} = F(E_{CM})$; moreover, $K_0(\mathcal{O}_{\varepsilon_n}) \cong E_{CM}(\mathbb{F}_{p^n})$.*

Note, that the second part of theorem 1 yields a localization of the $\mathbb{A}_{RM}$ at the prime p. Thus, the Cuntz-Krieger algebra can be interpreted as elliptic curve over a finite field; this fact is in line with the ideas of continuous geometry [8]. The formula $K_0(\mathcal{O}_{\varepsilon_n}) \cong E_{CM}(\mathbb{F}_{p^n})$ gives a new method of evaluation of the number of points of elliptic curve over the finite field (and all its extensions); all one needs to know is the matrix A at the LHS of the equation.

The structure of the text is as follows. Section 1 is reserved for a brief introduction to notation and basic facts needed to understand the article; theorem 1 is proved in section 2.

1 Preliminaries

1.1 The Grössencharacter

A. The complex multiplication. Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be a lattice in the complex plane $\mathbb{C}$. Recall that Λ defines an elliptic curve $E(\mathbb{C}) : y^2 =$

$4x^3 - g_2x - g_3$ via the complex analytic map $\mathbb{C}/\Lambda \to E(\mathbb{C})$ given by the formula $z \mapsto (\wp(z,\Lambda), \wp'(z,\Lambda))$, where $g_2 = 60\sum_{\omega\in\Lambda^\times}\omega^{-4}$, $g_3 = 140\sum_{\omega\in\Lambda^\times}\omega^{-6}$, $\Lambda^\times = \Lambda - \{0\}$ and $\wp(z,\Lambda) = z^{-2} + \sum_{\omega\in\Lambda^\times}((z-\omega)^{-2} - \omega^{-2})$ is the Weierstrass $\wp$ function. We shall further identify the elliptic curves $E(\mathbb{C})$ with the complex tori $\mathbb{C}/\Lambda$. If $\tau = \omega_2/\omega_1$ (a complex modulus), then $E_\tau(\mathbb{C}), E_{\tau'}(\mathbb{C})$ are isomorphic whenever $\tau' \equiv \tau \ mod\ SL_2(\mathbb{Z})$. Recall, that if Λ is a lattice in the complex plane $\mathbb{C}$, then the endomorphism ring $End\ (\Lambda)$ is isomorphic either to $\mathbb{Z}$ or to an order, R, in the imaginary quadratic number field k [11]. In the second case, the lattice is said to have a *complex multiplication*. We shall denote the corresponding elliptic curve by E_{CM}. Consider the cubic $E_\lambda : y^2 = x(x-1)(x-\lambda),\ \lambda \in \mathbb{C} - \{0,1\}$. The j-invariant of E_λ is given by the formula $j(E_\lambda) = 2^6(\lambda^2-\lambda+1)^3\lambda^{-2}(\lambda-1)^{-2}$. To find λ corresponding to the E_{CM}, one has to solve the polynomial equation $j(E_{CM}) = j(E_\lambda)$ with respect to λ. Since $j(E_{CM})$ is an algebraic integer ([11], p.38, Prop.4.5 b), the $\lambda_{CM} \in K$, where K is an algebraic extension (of the degree at most six) of the field $\mathbb{Q}(j(E_{CM}))$. Thus, each E_{CM} is isomorphic to a cubic $y^2 = x(x-1)(x-\lambda_{CM})$ defined over the field K. We shall write this fact as $E_{CM} \cong E(K)$.

B. The Hasse-Weil L-function. Let K be a number field and $E(K)$ an elliptic curve over K. For each prime ideal $\mathfrak{P}$ of K, let $\mathbb{F}_\mathfrak{P}$ be a residue field of K at $\mathfrak{P}$ and $q_\mathfrak{P} = N_\mathbb{Q}^K\mathfrak{P} = \#\mathbb{F}_\mathfrak{P}$, where $N_\mathbb{Q}^K$ is the norm of the ideal $\mathfrak{P}$. If $E(K)$ has a good reduction at $\mathfrak{P}$, one defines $a_\mathfrak{P} = q_\mathfrak{P} + 1 - \#\tilde{E}(\mathbb{F}_\mathfrak{P})$, where $\tilde{E}$ is a reduction of E modulo the prime ideal $\mathfrak{P}$. If E has good reduction at $\mathfrak{P}$, the polynomial $L_\mathfrak{P}(E(K),T) = 1 - a_\mathfrak{P}T + q_\mathfrak{P}T^2$, is called the *local L-series* of $E(K)$ at $\mathfrak{P}$. If E has bad reduction at $\mathfrak{P}$, the local L-series are $L_\mathfrak{P}(E(K),T) = 1 - T$ (resp. $L_\mathfrak{P}(E(K),T) = 1 + T$; $L_\mathfrak{P}(E(K),T) = 1$) if E has split multiplicative reduction at $\mathfrak{P}$ (if E has non-split multiplicative reduction at $\mathfrak{P}$; if E has additive reduction at $\mathfrak{P}$). The global L-series defined by the Euler product $L(E(K),s) = \prod_\mathfrak{P}[L_\mathfrak{P}(E(K), q_\mathfrak{P}^{-s})]^{-1}$, is called a *Hasse-Weil L-function* of the elliptic curve $E(K)$.

C. The Grössencharacter. Let A_K^* be the idele group of the number field K. A continuous homomorphism $\psi : A_K^* \to \mathbb{C}^*$ with the property $\psi(K^*) = 1$ is called a *Grössencharacter* on K. (The asterisk denotes the group of invertible elements of the corresponding ring.) The *Hecke L-series* attached to the Grössencharacter $\psi : A_K^* \to \mathbb{C}^*$ is defined by the Euler product $L(s,\psi) = \prod_\mathfrak{P}(1 - \psi(\mathfrak{P})q_\mathfrak{P}^{-s})^{-1}$, where the product is taken over all prime ideals of K.

D. The Deuring theorem. Let $E_{CM} \cong E(K)$ be an elliptic curve with complex multiplication by the ring of integers R of an imaginary quadratic field k, and assume that $K \supset k$. Let $\mathfrak{P}$ be a prime ideal of K at which $E(K)$ has a good reduction. If $\tilde{E}$ is a reduction of $E(K)$ at $\mathfrak{P}$, we let $\phi_{\mathfrak{P}} : \tilde{E} \to \tilde{E}$ be the associated Fröbenius map. Finally, let $\psi_{E(K)} : A_K^* \to k^*$ be the Grössencharacter attached to the E_{CM} (see [11], p.168). The following diagram is known to be commutative:

$$\begin{array}{ccc} E(K) & \xrightarrow{\psi_{E(K)}(\mathfrak{P})} & E(K) \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\phi_{\mathfrak{P}}} & \tilde{E} \end{array}$$

see [11], p.174. In particular, $\psi_{E(K)}(\mathfrak{P})$ is an endomorphism of the $E(K)$ given by the complex number $\alpha_{E(K)}(\mathfrak{P}) \in R$. By $\overline{\psi}_{E(K)}(\mathfrak{P})$ one understand the conjugate Grössencharacter viewed as a complex number. The *Deuring Theorem* says that the Hasse-Weil L-function of the $E(K)$ is related to the Hecke L-series of the $\psi_{E(K)}$ by the formula $L(E(K), s) \equiv L(s, \psi_{E(K)})L(s, \overline{\psi}_{E(K)})$.

1.2 Operator algebras

A. The C^*-algebras. The C^*-algebra is an algebra A over $\mathbb{C}$ with a norm $a \mapsto ||a||$ and an involution $a \mapsto a^*$ such that it is complete with respect to the norm and $||ab|| \leq ||a||\ ||b||$ and $||a^*a|| = ||a^2||$ for all $a, b \in A$. If A is commutative, then the Gelfand theorem says that A is isomorphic to the C^*-algebra $C_0(X)$ of continuous complex-valued functions on a locally compact Hausdorff space X. For otherwise, A represents a noncommutative topological space X. Let A be a C^*-algebra deemed as a noncommutative topological space. One can ask when two such topological spaces A, A' are homeomorphic? To answer the question, let us recall the topological K-theory. If X is a (commutative) topological space, denote by $V_{\mathbb{C}}(X)$ an abelian monoid consisting of the isomorphism classes of the complex vector bundles over X endowed with the Whitney sum. The abelian monoid $V_{\mathbb{C}}(X)$ can be made to an abelian group, $K(X)$, using the Grothendieck completion. The covariant functor $F : X \to K(X)$ is known to map the homeomorphic topological spaces X, X' to the isomorphic abelian groups

$K(X), K(X')$. Let now A, A' be the C^*-algebras. If one wishes to define a homeomorphism between the noncommutative topological spaces A and A', it will suffice to define an isomorphism between the abelian monoids $V_{\mathbb{C}}(A)$ and $V_{\mathbb{C}}(A')$ as suggested by the topological K-theory. The rôle of the complex vector bundle of degree n over the C^*-algebra A is played by a C^*-algebra $M_n(A) = A \otimes M_n$, i.e. the matrix algebra with the entries in A. The abelian monoid $V_{\mathbb{C}}(A) = \cup_{n=1}^{\infty} M_n(A)$ replaces the monoid $V_{\mathbb{C}}(X)$ of the topological K-theory. Therefore, the noncommutative topological spaces A, A' are homeomorphic, if $V_{\mathbb{C}}(A) \cong V_{\mathbb{C}}(A')$ are isomorphic abelian monoids. The latter equivalence is called a *stable isomorphism* of the C^*-algebras A and A' and is formally written as $A \otimes \mathcal{K} \cong A' \otimes \mathcal{K}$, where $\mathcal{K} = \cup_{n=1}^{\infty} M_n$ is the C^*-algebra of compact operators. Roughly speaking, the stable isomorphism between the C^*-algebras A and A' means that A and A' are homeomorphic as the noncommutative topological spaces.

B. The AF-algebras. An *AF-algebra* (approximately finite C^*-algebra) is defined to be the norm closure of an ascending sequence of the finite dimensional C^*-algebras M_n's, where M_n is the C^*-algebra of the $n \times n$ matrices with the entries in $\mathbb{C}$. Here the index $n = (n_1, \ldots, n_k)$ represents a semi-simple matrix algebra $M_n = M_{n_1} \oplus \ldots \oplus M_{n_k}$. The ascending sequence mentioned above can be written as $M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \ldots$, where M_i are the finite dimensional C^*-algebras and φ_i the homomorphisms between such algebras. The set-theoretic limit $A = \lim M_n$ has a natural algebraic structure given by the formula $a_m + b_k \to a + b$; here $a_m \to a, b_k \to b$ for the sequences $a_m \in M_m, b_k \in M_k$. The homomorphisms φ_i can be arranged into a graph as follows. Let $M_i = M_{i_1} \oplus \ldots \oplus M_{i_k}$ and $M_{i'} = M_{i'_1} \oplus \ldots \oplus M_{i'_k}$ be the semi-simple C^*-algebras and $\varphi_i : M_i \to M_{i'}$ the homomorphism. One has the two sets of vertices $V_{i_1}, \ldots, V_{i_k}$ and $V_{i'_1}, \ldots, V_{i'_k}$ joined by the a_{rs} edges, whenever the summand M_{i_r} contains a_{rs} copies of the summand $M_{i'_s}$ under the embedding φ_i. As i varies, one obtains an infinite graph called a *Bratteli diagram* of the AF-algebra.

C. The dimension group. Let A be a unital C^*-algebra and $V(A)$ be the union (over n) of projections in the $n \times n$ matrix C^*-algebra with entries in A. Projections $p, q \in V(A)$ are equivalent if there exists a partial isometry u such that $p = u^*u$ and $q = uu^*$. The equivalence class of projection p is denoted by $[p]$. The equivalence classes of orthogonal projections can be made to a semigroup by putting $[p] + [q] = [p + q]$. The Grothendieck completion of this semigroup to an abelian group is called a K_0-group of

algebra A. Functor $A \to K_0(A)$ maps a category of unital C^*-algebras into the category of abelian groups so that projections in algebra A correspond to a positive cone $K_0^+ \subset K_0(A)$ and the unit element $1 \in A$ corresponds to an order unit $u \in K_0(A)$. The ordered abelian group (K_0, K_0^+, u) with an order unit is called a *dimension group*. For example, let $\mathbb{A}_\theta$ be a noncommutative torus, i.e. an AF-algebra given by the Bratteli diagram of Fig. 1. It is known that $K_0(\mathbb{A}_\theta) \cong \mathbb{Z}^2$ and $K_0^+(\mathbb{A}_\theta) = \{(p,q) \in \mathbb{Z}^2 \mid p + \theta q \geq 0\}$. The AF-algberas $\mathbb{A}_\theta, \mathbb{A}_{\theta'}$ are stably isomorphic, i.e. $\mathbb{A}_\theta \otimes \mathcal{K} \cong \mathbb{A}_{\theta'} \otimes \mathcal{K}$, if and only if $\mathbb{Z} + \theta\mathbb{Z} = \mathbb{Z} + \theta'\mathbb{Z}$ as the subsets of $\mathbb{R}$. It is common to call $\mathbb{Z} + \theta\mathbb{Z}$ a *pseudo-lattice* [7].

D. The Cuntz-Krieger algebra. A Cuntz-Krieger algebra, $\mathcal{O}_B$, is the C^*-algebra generated by partial isometries $s_1, \ldots, s_n$ that act on a Hilbert space in such a way that their support projections $Q_i = s_i^* s_i$ and their range projections $P_i = s_i s_i^*$ are orthogonal and satisfy the relations $Q_i = \sum_{j=i}^n a_{ij} P_j$, for an $n \times n$ matrix $B = (b_{ij})$ consisting of 0's and 1's [3]. The notion is extendable to the matrices B with the non-negative integer entries *ibid., Remark 2.16.* It is known, that the C^*-algebra $\mathcal{O}_B$ is simple, whenever matrix B is irreducible (i.e. a certain power of B is a strictly positive integer matrix). It was established in [3], that $K_0(\mathcal{O}_B) \cong \mathbb{Z}^n/(I - B^t)\mathbb{Z}^n$ and $K_1(\mathcal{O}_B) = Ker\ (I - B^t)$, where B^t is a transpose of the matrix B. It is not difficult to see, that whenever $det\ (I - B^t) \neq 0$, the $K_0(\mathcal{O}_B)$ is a finite abelian group and $K_1(\mathcal{O}_B) = 0$. The both groups are invariants of the stable isomorphism class of the Cuntz-Krieger algebra.

2 Proof of theorem 1

Let p be such, that E_{CM} has a good reduction at $\mathfrak{P}$; the corresponding local zeta function $\zeta_p(E_{CM}, z) = (1 - tr\ (\psi_{E(K)}(\mathfrak{P}))z + pz^2)^{-1}$, where $\psi_{E(K)}$ is the Grössencharacter on K and tr is the trace of algebraic number. We have to prove, that $\zeta_p(E_{CM}, z) = \zeta_p(\mathbb{A}_{RM}, z) := (1 - tr\ (A^p)z + pz^2)^{-1}$; the last equality is a consequence of definition of $\zeta_p(\mathbb{A}_{RM}, z)$. Roughly speaking, our proof consists in construction of representation ρ of $\psi_{E(K)}$ into the group of invertible elements (units) of $End\ (K_0(\mathbb{A}_{RM}))$, such that:

$$tr\ (\psi_{E(K)}(\mathfrak{P})) = tr\ (\rho(\psi_{E(K)}(\mathfrak{P}))) = tr\ (A^p). \qquad (1)$$

This will be achieved with the help of an explicit formula ([9], p.524) for the Teichmüller functor F:

$$F : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in End\ (E_{CM}) \longmapsto \begin{pmatrix} a & b \\ -c & -d \end{pmatrix} \in End\ (K_0(\mathbb{A}_{RM})). \qquad (2)$$

We shall split the proof into a series of lemmas, starting with the following simple

Lemma 1 *Let $A = (a, b, c, d)$ be an integer matrix with $ad - bc \neq 0$ and $b = 1$. Then A is similar to the matrix $(a + d, 1, c - ad, 0)$.*

Proof. Indeed, take a matrix $(1, 0, d, 1) \in SL_2(\mathbb{Z})$. The matrix realizes the similarity, i.e.

$$\begin{pmatrix} 1 & 0 \\ -d & 1 \end{pmatrix} \begin{pmatrix} a & 1 \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix} = \begin{pmatrix} a + d & 1 \\ c - ad & 0 \end{pmatrix}. \quad \square \qquad (3)$$

Lemma 2 *The matrix $A = (a + d, 1, c - ad, 0)$ is similar to its transpose $A^t = (a + d, c - ad, 1, 0)$.*

Proof. We shall use the following criterion: the (integer) matrices A and B are similar, if and only if the characteristic matrices $xI - A$ and $xI - B$ have the same Smith normal form. The calculation for the matrix $xI - A$ gives:

$$\begin{pmatrix} x - a - d & -1 \\ ad - c & x \end{pmatrix} \sim \begin{pmatrix} x - a - d & -1 \\ x^2 - (a + d)x + ad - c & 0 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 \\ 0 & x^2 - (a + d)x + ad - c \end{pmatrix},$$

where $\sim$ are the elementary operations between the rows (columns) of the matrix. Similarly, a calculation for the matrix $xI - A^t$ gives:

$$\begin{pmatrix} x - a - d & ad - c \\ -1 & x \end{pmatrix} \sim \begin{pmatrix} x - a - d & x^2 - (a + d)x + ad - c \\ -1 & 0 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 \\ 0 & x^2 - (a + d)x + ad - c \end{pmatrix}.$$

Thus, $(xI - A) \sim (xI - A^t)$ and lemma 2 follows. $\square$

Corollary 1 *The matrices* $(a, 1, c, d)$ *and* $(a + d, c - ad, 1, 0)$ *are similar.*

Proof. It follows from lemmas 1-2. □

Let E_{CM} be elliptic curve with the complex multiplication by an order R in the ring of integers of the imaginary quadratic field k. Then $\mathbb{A}_{RM} = F(E_{CM})$ is a noncommutative torus with real multiplication by the order $\mathfrak{R}$ in the ring of integers of a real quadratic field $\mathfrak{k}$. Let $tr\ (\alpha) = \alpha + \bar{\alpha}$ be the trace function of a (quadratic) algebraic number field.

Lemma 3 *Each* $\alpha \in R$ *goes under* F *into an* $\omega \in \mathfrak{R}$*, such that* $tr\ (\alpha) = tr\ (\omega)$.

Proof. Recall that each $\alpha \in R$ can be written in a matrix form for a given base $\{\omega_1, \omega_2\}$ of the lattice Λ. Namely,

$$\left\{ \begin{array}{ll} \alpha\omega_1 & = a\omega_1 + b\omega_2 \\ \alpha\omega_2 & = c\omega_1 + d\omega_2, \end{array} \right. \tag{4}$$

where (a, b, c, d) is an integer matrix with $ad - bc \neq 0$. Note that $tr\ (\alpha) = a + d$ and $b\tau^2 + (a - d)\tau - c = 0$, where $\tau = \omega_2/\omega_1$. Since τ is an algebraic integer, we conclude that $b = 1$.

In view of corollary 1, in a base $\{\omega_1', \omega_2'\}$, the α has a matrix form $(a + d, c - ad, 1, 0)$.

To calculate a real quadratic $\omega \in \mathfrak{R}$ corresponding to α, recall an explicit formula from [9]. Namely, the functor F maps every endomorphism (a, b, c, d) of the lattice $\mathbb{Z} + \mathbb{Z}\tau$ to an endomorphism $(a, b, -c, -d)$ of the pseudo-lattice $\mathbb{Z} + \mathbb{Z}\theta$ *ibid. p.524.* Thus, one gets:

$$F : \begin{pmatrix} a + d & c - ad \\ 1 & 0 \end{pmatrix} \longmapsto \begin{pmatrix} a + d & c - ad \\ -1 & 0 \end{pmatrix}. \tag{5}$$

In other words, for a given base $\{\lambda_1, \lambda_2\}$ of the pseudo-lattice $\mathbb{Z} + \mathbb{Z}\theta$ one can write

$$\left\{ \begin{array}{ll} \omega\lambda_1 & = (a + d)\lambda_1 + (c - ad)\lambda_2 \\ \omega\lambda_2 & = -\lambda_1. \end{array} \right. \tag{6}$$

It is an easy exercise to verify that ω is a real quadratic integer with $tr\ (\omega) = a + d$. The latter coincides with the $tr\ (\alpha)$. □

Let $\omega \in \mathfrak{R}$ be an endomorphism of the pseudo-lattice $\mathbb{Z} + \mathbb{Z}\theta$ of degree $deg\ (\omega) := \omega\bar{\omega} = n$. The endomorphism maps the pseudo-lattice to a sub-lattice of index n. Any such has a form $\mathbb{Z} + (n\theta)\mathbb{Z}$ [2], p.131.

Let us calculate ω in a base $\{1, n\theta\}$, when ω is given by the matrix $(a+d, c-ad, -1, 0)$. In this case $n = c - ad$ and ω induces an automorphism $\omega^* = (a+d, 1, -1, 0)$ of the sublattice $\mathbb{Z} + (n\theta)\mathbb{Z}$ according to the matrix equation:

$$\begin{pmatrix} a+d & n \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \theta \end{pmatrix} = \begin{pmatrix} a+d & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ n\theta \end{pmatrix}. \tag{7}$$

Thus, one gets a map $\rho : \mathfrak{R} \to \mathfrak{R}^*$ given by the formula $\omega = (a+d, n, -1, 0) \mapsto \omega^* = (a+d, 1, -1, 0)$, where $\mathfrak{R}^*$ is the group of units of the $\mathfrak{R}$.

Lemma 4 *$tr\ (\omega) = tr\ (\rho(\omega)),\ \forall \omega \in \mathfrak{R}$.*

Proof. Note, that $tr\ (\omega^*) = a + d = tr\ (\omega)$. Since $\omega^* = \rho(\omega)$, lemma 4 follows. □

Note, that $\mathfrak{R}^* = \{\pm\varepsilon^k \mid k \in \mathbb{Z}\}$, where $\varepsilon > 1$ is a fundamental unit of the order $\mathfrak{R} \subseteq O_{\mathfrak{k}}$; here $O_{\mathfrak{k}}$ means the ring of integers of a real quadratic field $\mathfrak{k} = \mathbb{Q}(\theta)$. Choosing a sign in front of ε^k, the following index map is defined:

$$\iota : R \xrightarrow{\text{F}} \mathfrak{R} \xrightarrow{\rho} \mathfrak{R}^* \longrightarrow \mathbb{Z}. \tag{8}$$

Let $\alpha \in R$ and $deg\ (\alpha) = -n$. To calculate the $\iota(\alpha)$, let us recall some notation from Hasse [6], §16.5.C. Let $\mathbb{Z}_n$ be a cyclic group of order n. For brevity, let $I = \mathbb{Z} + \mathbb{Z}\theta$ be a pseudo-lattice and $I_n = \mathbb{Z} + (n\theta)\mathbb{Z}$ its sub-lattice of index n; the fundamental units of I and I_n are ε and ε_n, respectively. By $\mathfrak{G}_n$ one understands a subgroup of $\mathbb{Z}_n$ of prime residue classes *mod* n. The $\mathfrak{g}_n \subset \mathfrak{G}_n$ is a subgroup of the non-zero divisors of the $\mathfrak{G}_n$. Finally, let g_n be the smallest number, such that it divides $|\mathfrak{G}_n/\mathfrak{g}_n|$ and $\varepsilon^{g_n} \in I_n$. (The notation drastically simplifies in the case $n = p$ is a prime number.)

Lemma 5 *$\iota(\alpha) = g_n$.*

Proof. First note, that $deg\ (\omega) = -deg\ (\alpha) = n$, where $\omega = F(\alpha)$. Then the map ρ defines I and I_n; one can now apply the calculation of [6], pp 296-300. Namely, **Theorem XIII'** on page 298 yields the required result. (We kept the notation of the original.) □

Corollary 2 *$\iota(\psi_{E(K)}(\mathfrak{P})) = p$.*

Proof. It is known, that $deg\ (\psi_{E(K)}(\mathfrak{P})) = -p$, where $\psi_{E(K)}(\mathfrak{P}) \in R$ is the Grössencharacter. To calculate the g_n in the case $n = p$, notice that the $\mathfrak{G}_p \cong \mathbb{Z}_p$ and $\mathfrak{g}_p$ is trivial. Thus, $|\mathfrak{G}_p/\mathfrak{g}_p| = p$ is divisible only by 1 or p. Since ε^1 is not in I_n, one concludes that $g_p = p$. The corollary follows. □

Lemma 6 *tr* $(\psi_{E(K)}(\mathfrak{P})) = tr\ (A^p)$.

Proof. It is not hard to see, that A is a hyperbolic matrix with the eigenvector $(1, \theta)$; the corresponding (Perron-Frobenius) eigenvalue is a fundamental unit $\varepsilon > 1$ of the pseudo-lattice $\mathbb{Z} + \mathbb{Z}\theta$. In other words, A is a matrix form of the algebraic number ε. It is immediate, that A^p is the matrix form for the ε^p and $tr\ (A^p) = tr\ (\varepsilon^p)$.

In view of lemmas 3 and 4, $tr\ (\alpha) = tr\ (F(\alpha)) = tr\ (\rho(F(\alpha)))$ for $\forall \alpha \in R$. In particular, if $\alpha = \psi_{E(K)}(\mathfrak{P})$ then, by corollary 2, one gets $\rho(F(\psi_{E(K)}(\mathfrak{P}))) = \varepsilon^p$. Taking traces in the last equation, we obtain the conclusion of lemma 6. □

One can finish the proof of theorem 1 by comparing the local L-series of the Hasse-Weil L-function for the E_{CM} with that of the local zeta for the $\mathbb{A}_{RM}$. The local L-series for E_{CM} are $L_{\mathfrak{P}}(E(K), T) = 1 - a_{\mathfrak{P}}T + q_{\mathfrak{P}}T^2$ if the E_{CM} has a good reduction at $\mathfrak{P}$ and $L_{\mathfrak{P}}(E(K), T) = 1 - \alpha T$ otherwise; here

$$\begin{array}{rcl} q_{\mathfrak{P}} & = & N_{\mathbb{Q}}^{K}\mathfrak{P} = \#\mathbb{F}_{\mathfrak{P}} = p, \\ a_{\mathfrak{P}} & = & q_{\mathfrak{P}} + 1 - \#\tilde{E}(\mathbb{F}_{\mathfrak{P}}) = tr\ (\psi_{E(K)}(\mathfrak{P})), \\ \alpha & \in & \{-1, 0, 1\}. \end{array} \tag{9}$$

Therefore,

$$L_{\mathfrak{P}}(E_{CM}, T) = \begin{cases} 1 - tr\ (\psi_{E(K)}(\mathfrak{P}))T + pT^2, & \text{for good reduction} \\ 1 - \alpha T, & \text{for bad reduction.} \end{cases} \tag{10}$$

Let now $\mathbb{A}_{RM} = F(E_{CM})$. The following remark will greatly simplify our calculations.

Remark 1 *The matrix L_p is similar to the matrix $(tr\ (A^p), p, -1, 0)$; with an abuse, we shall use the notation $L_p = (tr\ (A^p), p, -1, 0)$ till the end of the proof.*

Lemma 7 $\zeta_p^{-1}(\mathbb{A}_{RM}, T) = 1 - tr\ (A^p)T + pT^2$, *whenever* $p \nmid tr^2(A) - 4$.

Proof. By the formula $K_0(\mathcal{O}_B) = \mathbb{Z}^2/(I - B^t)\mathbb{Z}^2$, one gets:

$$|K_0(\mathcal{O}_{L_p^n})| = \left| \frac{\mathbb{Z}^2}{(I - (L_p^n)^t)\mathbb{Z}^2} \right| = |det(I - (L_p^n)^t)| = |Fix\ (L_p^n)|, \tag{11}$$

where $Fix\ (L_p^n)$ is the set of (geometric) fixed points of the endomorphism $L_p^n : \mathbb{Z}^2 \to \mathbb{Z}^2$. Thus,

$$\zeta_p(\mathbb{A}_{RM}, z) = \exp\left(\sum_{n=1}^{\infty} \frac{|Fix\ (L_p^n)|}{n}\ z^n\right), \quad z \in \mathbb{C}. \tag{12}$$

But the latter series is an Artin-Mazur zeta function of the endomorphism L_p; it converges to a rational function $det^{-1}(I - zL_p)$ [5], p.455. Thus, $\zeta_p(\mathbb{A}_{RM}, z) = det^{-1}(I - zL_p)$.

The substitution $L_p = (tr\ (A^p), p, -1, 0)$ gives us:

$$det\ (I - zL_p) = det\ \begin{pmatrix} 1 - tr\ (A^p)z & -pz \\ z & 1 \end{pmatrix} = 1 - tr\ (A^p)z + pz^2. \tag{13}$$

Put $z = T$ and get $\zeta_p(\mathbb{A}_{RM}, T) = (1 - tr\ (A^p)T + pT^2)^{-1}$, which is a conclusion of lemma 7. □

Lemma 8 *$\zeta_p^{-1}(\mathbb{A}_{RM}, T) = 1 - \alpha T$, whenever $p \mid tr^2(A) - 4$.*

Proof. Indeed, $K_0(\mathcal{O}_{1-\alpha^n}) = \mathbb{Z}/(1 - 1 + \alpha^n)\mathbb{Z} = \mathbb{Z}/\alpha^n\mathbb{Z}$. Thus, $|K_0(\mathcal{O}_{1-\alpha^n})| = det\ (\alpha^n) = \alpha^n$. By the definition,

$$\zeta_p(\mathbb{A}_{RM}, z) = \exp\left(\sum_{n=1}^{\infty} \frac{\alpha^n}{n} z^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{(\alpha z)^n}{n}\right) = \frac{1}{1 - \alpha z}. \tag{14}$$

The substitution $z = T$ gives a conclusion of lemma 8. □

Lemma 9 *Let p be a prime, such that $p \mid tr^2(A) - 4$; let $\mathfrak{P} \subset K$ be a prime ideal over p. Then $E_{CM} = E(K)$ has a bad reduction at $\mathfrak{P}$.*

Proof. Let k be a field of complex multiplication of the E_{CM}; its discriminant we shall write as $\Delta_k < 0$. It is known, that whenever $p \mid \Delta_k$, the E_{CM} has a bad reduction at the prime ideal $\mathfrak{P}$ over p.

On the other hand, the explicit formula (2) applied to the matrix L_p gives us $F : (tr\ (A^p), p, -1, 0) \mapsto (tr\ (A^p), p, 1, 0)$. The characteristic polynomials of the above matrices are $x^2 - tr\ (A^p)x + p$ and $x^2 - tr\ (A^p)x - p$, respectively. They generate an imaginary (resp., a real) quadratic field k (resp., $\mathfrak{k}$) with the discriminant $\Delta_k = tr^2(A^p) - 4p < 0$ (resp., $\Delta_{\mathfrak{k}} = tr^2(A^p) + 4p > 0$). Thus, $\Delta_{\mathfrak{k}} - \Delta_k = 8p$. It is easy to see, that if $p \mid \Delta_{\mathfrak{k}}$, then $p \mid \Delta_k$ as well. It remains to express the discriminant $\Delta_{\mathfrak{k}}$ in terms of the matrix A. Since the characteristic

polynomial for A is $x^2 - tr\ (A)x + 1$, it follows that $\Delta_{\mathfrak{k}} = tr^2(A) - 4$. Thus, if $p \mid tr^2(A) - 4$, then $p \mid \Delta_k$, i.e. p is a bad prime. $\square$

We are prepared now to prove the first part of theorem 1. Note, that a critical piece of information is provided by lemma 6, which says that $tr\ (\psi_{E(K)}(\mathfrak{P})) = tr\ (A^p)$. Thus, in view of lemmas 7-9, $L_{\mathfrak{P}}(E_{CM}, T) \equiv \zeta_p^{-1}(\mathbb{A}_{RM}, T)$. The first part of theorem 1 follows.

A. Let p be a good prime. Let us prove the second part of theorem 1 in the case $n = 1$. From the left side: $K_0(\mathbb{A}_{RM} \rtimes_{L_p} \mathbb{Z}) \cong K_0(\mathcal{O}_{L_p}) \cong \mathbb{Z}^2/(I - L_p^t)\mathbb{Z}^2$, where $L_p = (tr\ (A^p), p, -1, 0)$. To calculate the abelian group $\mathbb{Z}^2/(I - L_p^t)\mathbb{Z}^2$, we shall use a reduction of the matrix $I - L_p^t$ to the Smith normal form:

$$I - L_p^t = \begin{pmatrix} 1 - tr\ (A^p) & 1 \\ -p & 1 \end{pmatrix} \sim \begin{pmatrix} 1 + p - tr\ (A^p) & 0 \\ -p & 1 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 \\ 0 & 1 + p - tr\ (A^p) \end{pmatrix}.$$

Therefore, $K_0(\mathcal{O}_{L_p}) \cong \mathbb{Z}_{1+p-tr\ (A^p)}$.

From the right side, the $E_{CM}(\mathbb{F}_{\mathfrak{P}})$ is an elliptic curve over the field of characteristic p. Recall, that the chord and tangent law turns the $E_{CM}(\mathbb{F}_{\mathfrak{P}})$ into a finite abelian group. The group is cyclic and has the order $1 + q_{\mathfrak{P}} - a_{\mathfrak{P}}$ (§3.1.B). But $q_{\mathfrak{P}} = p$ and $a_{\mathfrak{P}} = tr\ (\psi_{E(K)}(\mathfrak{P})) = tr\ (A^p)$ (lemma 6). Thus, $E_{CM}(\mathbb{F}_{\mathfrak{P}}) \cong \mathbb{Z}_{1+p-tr\ (A^p)}$; therefore $K_0(\mathcal{O}_{L_p}) \cong E_{CM}(\mathbb{F}_p)$.

The general case $n \geq 1$ is treated likewise. Repeating the argument of lemmas 1-2, it follows that $L_p^n = (tr\ (A^{pn}, p^n, -1, 0)$. Then one gets $K_0(\mathcal{O}_{L_p^n}) \cong \mathbb{Z}_{1+p^n-tr\ (A^{pn})}$ on the left side. From the right side, $|E_{CM}(\mathbb{F}_{p^n})| = 1 + p^n - tr\ (\psi_{E(K)}^n(\mathfrak{P}))$; but a repetition of the argument of lemma 6 yields us $tr\ (\psi_{E(K)}^n(\mathfrak{P})) = tr\ (A^{pn})$. Comparing the left and right sides, one gets that $K_0(\mathcal{O}_{L_p^n}) \cong E_{CM}(\mathbb{F}_{p^n})$. This argument finishes the proof of the second part of theorem 1 for the good primes.

B. Let p be a bad prime. From the proof of lemma 8, one gets for the left side $K_0(\mathcal{O}_{\varepsilon_n}) \cong \mathbb{Z}_{\alpha^n}$. From the right side, it holds $|E_{CM}(\mathbb{F}_{p^n})| = 1 + q_{\mathfrak{P}} - a_{\mathfrak{P}}$, where $q_{\mathfrak{P}} = 0$ and $a_{\mathfrak{P}} = tr\ (\varepsilon_n) = \varepsilon_n$. Thus, $|E_{CM}(\mathbb{F}_{p^n})| = 1 - \varepsilon_n = 1 - (1 - \alpha^n) = \alpha^n$. Comparing the left and right sides, we conclude that $K_0(\mathcal{O}_{\varepsilon_n}) \cong E_{CM}(\mathbb{F}_{p^n})$ at the bad primes.

All cases are exhausted; thus, theorem 1 is proved. $\square$

References

[1] B. Blackadar, K-Theory for Operator Algebras, MSRI Publications, Springer, 1986.

[2] Z. I. Borevich and I. R. Shafarevich, Number Theory, Acad. Press, 1966.

[3] J. Cuntz and W. Krieger, A class of C^*-algebras and topological Markov chains, Invent. Math. 56 (1980), 251-268.

[4] E. Effros and C.-L. Shen, Approximately finite C^*-algebras and continued fractions, Indiana J. Math. 29 (1980), 191-204.

[5] R. Hartshorn, Algebraic Geometry, GTM 52, Springer, 1977.

[6] H. Hasse, Vorlesungen über Zahlentheorie, Springer, 1950.

[7] Yu. I. Manin, Real multiplication and noncommutative geometry, in "Legacy of Niels Hendrik Abel", 685-727, Springer, 2004.

[8] J. von Neumann, Continuous Geometry, Princeton Univ. Press, Princeton, New Jersey, 1960.

[9] I. Nikolaev, Remark on the rank of elliptic curves, Osaka J. Math. 46 (2009), 515-527.

[10] M. Pimsner and D. Voiculescu, Imbedding the irrational rotation C^*-algebra into an AF-algebra, J. Operator Theory 4 (1980), 201-210.

[11] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, GTM 151, Springer 1994.

The Fields Institute for Mathematical Sciences, Toronto, ON, Canada, E-mail: igor.v.nikolaev@gmail.com

Current address: 101-315 Holmwood Ave., Ottawa, ON, Canada, K1S 2R2